I oppose this snooping on VoIP calls as pointless and simply an intrusion into law-abiding citizens. For technical reasons (I am a senior research engineer focused on internet technologies), I do not believe that this will bear fruit in terrorism or in crime.

Let's use an analogy. The government passed a law to ban certain automatic assault weapons (although some of that is now gone). I support that. While it doesn't prevent criminals from gaining access to guns, it certainly makes it harder. This works with physical assets. This doesn't work with software assets. Anybody with a trace of software skills can write an un-crackable VoIP software plugin to click into any existing VoIP codebase they can get their hands on. Open source encryption tools are widely available and by using low-tech means for key distribution (e.g. hand carrying the public key on a card), there simply are no linch points in the design. For a terrorist organization to outfit its entire network with this VoIP software requires merely posting it to a couple sites or fileshares under a discrete name. Even with access to the ISP (I work in an ISP as part of my job), that traffic is not decryptable. In fact, by being clever with the traffic shaping and port use, it would be quite easy to make the transmission look like any standard HTTPS (secure webpage) transaction. Thus it effectively looks like someone is checking their bank records, or sending an email from their secure web-based mail server when in fact they are having a brief encrypted phone call.

Due to the propogation of software, due to the restricted "network" created between the few criminals in the outfit, and due to the ability for calls to originate and terminate from many locations, I can't see how snooping in at ISPs and forcing reputable VoIP software makers to insert weaknesses into their software encryption solves any of this.

I am sure there is a real and important goal that you are trying to achieve here. I ask that you reconsider the age we are in and the technology that you are up against and come up with a more effective solution.

Brent Elliott